WHAT IS CLAIMED IS:

1. A method for accessing a memory storage device, the memory storage device being in communication with a host system through an adapter, the memory storage device including a memory, the method comprising:

obtaining a key from the adapter, the key being arranged to encrypt information that is arranged to be stored in the memory, the key further being arranged to decrypt the encrypted information, wherein the key is substantially stored on the adapter; and

processing the information using the key.

2. The method of claim 1 wherein the information is stored in the memory, and the method further includes:

obtaining the information that is stored in the memory, wherein processing the information using the key includes decrypting the information using the key.

3. The method of claim 1 wherein the information is provided by the host system, and processing the information using the key includes encrypting the information using the key.

4. The method of claim 3 further including:

storing the encrypted information in the memory.

5. The method of claim 1 wherein obtaining the key from the adapter includes:

providing a first password to the adapter;

determining when the first password is valid; and

decoding contents associated with the adapter using the first password when it is determined that the first password is valid, wherein the contents include the key.

6. The method of claim 5 wherein determining when the first password is valid includes comparing the first password to a second password to determine if the first

password is substantially the same as the second password, wherein the second password is stored on the adapter.

7. The method of claim 1 wherein obtaining the key from the adapter includes:

providing a first password to the adapter;

generating a second password on the adapter using the first password;

determining when the second password is suitable for decoding contents associated with the adapter; and

decoding the contents using the second password when it is determined that the second password is suitable for decoding the contents associated with the adapter, wherein the contents include the key.

8. The method of claim 1 wherein the adapter includes a random access memory (RAM), and obtaining the key from the adapter includes:

providing a password to the RAM; and

decoding the contents using the password, wherein the contents include the key.

9. The method of claim 8 further including:

providing the decoded contents to the host computer.

10. The method of claim 1 wherein the memory storage device is a memory card that includes a non-volatile memory.

11. The method of claim 10 wherein the memory card is one selected from the group consisting of a secure digital card, a Compact Flash card, a multimedia card, a smart media card, and a Memory Stick card.

12. The method of claim 1 wherein the adapter is one of a Universal Serial Bus (USB) reader and a Personal Computer Memory Card International Association (PCMCIA) adapter.

13. A system comprising:

a memory storage device, the memory storage device including a memory; and

an adapter, the adapter being arranged to interface with the memory storage device, wherein the adapter is arranged to store a key that is associated with the memory storage device.

14. The system according to claim 13 further including:

a host, the host being in communication with the adapter such that the host may communicate with the memory storage device through the adapter.

15. The system according to claim 14 wherein the host includes:

means for accessing the key.

16. The system according to claim 15 wherein the means for accessing the key include means for providing a first password to the adapter, and the adapter includes means for receiving the first password and means for processing the first password.

17. The system according to claim 16 wherein the means for processing the first password include:

means for comparing the first password to a second password that is stored on the adapter;

means for determining when the first password substantially matches the second password;

means for substantially obtaining the key using the second password when it is determined that the first password substantially matches the second password such that the key may be accessed by the host.

18. The system according to claim 17 wherein the means for processing the first password include:

means for obtaining a second password using the first password substantially within the adapter;

means for determining when the second password is suitable for obtaining the key; and

means for substantially obtaining the key such that the key may be accessed by the host using the second password when the second password is determined to be suitable for obtaining the key.

19. The system according to claim 17 wherein the key is included in encoded contents associated with the adapter and the means for receiving the password include a random access memory (RAM), and wherein the means for processing the first password include:

means for decoding the encoded contents using the first password.

20. The system according to claim 14 wherein the host is arranged to encrypt information and to write the encrypted information into the memory through the adapter.

21. The system according to claim 14 wherein the host is arranged to read information from the memory through the adapter and to decrypt the information using the key.

22. The system according to claim 13 wherein the memory storage device is a memory card and the memory is a non-volatile memory.

23. The system according to claim 22 wherein the memory card is one selected from the group consisting of a secure digital card, a Compact Flash card, a multimedia card, and a Memory Stick card.

24. The system according to claim 13 wherein the adapter is one of a Universal Serial Bus (USB) reader and a Personal Computer Memory Card International Association (PCMCIA) adapter.

25. A reader comprising:

a receptacle, the receptacle being arranged to receive a memory card;

an interface, the interface being arranged to enable the reader to communicate with a host; and

an area, the area being arranged to store contents, wherein the contents are substantially password-protected.

26. The reader according to claim 25 wherein the contents include a key, the key being arranged to enable information to be substantially written to or substantially read from the memory card.

27. The reader according to claim 25 further including:

a password processing arrangement, the password processing arrangement being arranged to receive a password through the interface, wherein the contents are arranged to be retrieved from the area through the interface by the host when the received password is appropriate.

28. The reader according to claim 27 wherein the password processing arrangement is arranged to determine whether the received password is appropriate.

29. The reader according to claim 28 wherein the password processing arrangement is arranged to decode the contents when it is determined that the received password is appropriate substantially before the contents are retrieved through the interface by the host.

30. The reader according to claim 25 further including:

a random access memory (RAM); and

a password processing arrangement, the password processing arrangement being arranged to receive a password through the interface and to provide the password to the

RAM, wherein the contents are arranged to be substantially decoded using the password and retrieved through the interface by the host when the received password is appropriate.

31. The reader according to claim 25 wherein the reader is one of a Universal Serial Bus (USB) reader and a Personal Computer Memory Card International Association (PCMCIA) adapter.

32. A method for accessing protected contents on a reader, the reader being in communication with a host, wherein the reader is arranged to receive a memory card, the method comprising:

determining when functionality associated with supporting the protected contents is enabled on the reader; and

accessing a section of the reader that is arranged to store protected contents when it is determined that the functionality associated with supporting the protected contents is enabled.

33. The method of claim 32 wherein accessing the section of the reader that is arranged to store protected contents includes:

providing a data stream to the reader; and

writing the data stream into the section.

34. The method of claim 32 wherein accessing the section of the reader that is arranged to store protected contents includes:

encrypting a data stream;

providing the encrypted data stream to the reader; and

writing the encrypted data stream into the section.

35. The method of claim 32 wherein accessing the section of the reader that is arranged to store protected contents includes:

reading data from the section of the reader.

36. The method of claim 35 wherein accessing the section of the reader that is arranged to store protected contents further includes:

decrypting the data read from the section of the reader.

37. The method of claim 32 wherein determining when the functionality associated with supporting the protected contents is enabled includes:

providing a password to the reader.